Amendments to the Claims

1. (Currently amended) A method of transmitting contents information, comprising the steps of:

generating a first-key signal representative of a first key from first-key base information being a base of the first key;

encrypting contents information into encryption-resultant contents information in response to the first-key signal;

generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to one selected from a plurality of predetermined key generation algorithms;

encrypting at least a part of the first-key base information into encryption-resultant first-key base information in response to the second-key signal; and

transmitting the encryption-resultant contents information, the encryption-resultant first-key base information, the initial-value information, and algorithm identification information for identifying the one selected from the plurality of predetermined key generation algorithms ~~.~~;

wherein it is previously decided that the plurality of predetermined key generation algorithms are usable by a decrypting device in decryption of the encryption-resultant contents information, and the algorithm identification information is for identifying the one among the plurality of predetermined key generation algorithms which should be used by the decrypting device in response to a reference table holding the plurality of predetermined key generation algorithms.

2. (Currently amended) A method of recording contents information, comprising the steps of:

generating a first-key signal representative of a first key from first-key base information being a base of the first key;

encrypting contents information into encryption-resultant contents information in response to the first-key signal;

generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to one selected from a plurality of predetermined key generation algorithms;

encrypting at least a part of the first-key base information into encryption-resultant first-key base information in response to the second-key signal; and

recording the encryption-resultant contents information, the encryption-resultant first-key base information, the initial-value information, and algorithm identification information for identifying the one selected from the plurality of predetermined key generation algorithms~~.~~;

wherein it is previously decided that the plurality of predetermined key generation algorithms are usable by a decrypting device in decryption of the encryption-resultant contents information, and the algorithm identification information is for identifying the one among the plurality of predetermined key generation algorithms which should be used by the decrypting device in response to a reference table holding the plurality of predetermined key generation algorithms.

3. (Currently amended) An apparatus for transmitting contents information, comprising:

means for generating a first-key signal representative of a first key from first-key base information being a base of the first key;

means for encrypting contents information into encryption-resultant contents information in response to the first-key signal;

means for generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to one selected from a plurality of predetermined key generation algorithms;

means for encrypting at least a part of the first-key base information into encryption-resultant first-key base information in response to the second-key signal; and

means for transmitting the encryption-resultant contents information, the encryption-resultant first-key base information, the initial-value information, and algorithm identification information for identifying the one selected from the plurality of predetermined key generation algorithms~~.~~;

wherein it is previously decided that the plurality of predetermined key generation algorithms are usable by a decrypting device in decryption of the encryption-resultant contents information, and the algorithm identification information is for identifying the one among the plurality of predetermined key generation algorithms which should be used by the decrypting device in response to a reference table holding the plurality of predetermined key generation algorithms.

4. (Currently amended) An apparatus for recording contents information, comprising:

means for generating a first-key signal representative of a first key from first-key base information being a base of the first key;

means for encrypting contents information into encryption-resultant contents information in response to the first-key signal;

means for generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to one selected from a plurality of predetermined key generation algorithms;

means for encrypting at least a part of the first-key base information into encryption-resultant first-key base information in response to the second-key signal; and

means for recording the encryption-resultant contents information, the encryption-resultant first-key base information, the initial-value information, and algorithm identification information for identifying the one selected from the plurality of predetermined key generation algorithms~~.~~;

wherein it is previously decided that the plurality of predetermined key generation algorithms are usable by a decrypting device in decryption of the encryption-resultant contents information, and the algorithm identification information is for identifying the one among the plurality of predetermined key generation algorithms which should be used by the decrypting device in response to a reference table holding the plurality of predetermined key generation algorithms.

5. (Currently amended) A transmission medium for transmitting encryption-resultant contents information, encryption-resultant first-key base information, initial-value

information, and algorithm identification information, wherein the encryption-resultant contents information and the encryption-resultant first-key base information are generated by the steps of generating a first-key signal representative of a first key from first-key base information being a base of the first key; encrypting contents information into encryption-resultant contents information in response to the first-key signal; generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to one selected from a plurality of predetermined key generation algorithms; and encrypting at least a part of the first-key base information into encryption-resultant first-key base information in response to the second-key signal; and wherein the algorithm identification information is for identifying the one selected from the plurality of predetermined key generation algorithms~~.~~ ; and wherein it is previously decided that the plurality of predetermined key generation algorithms are usable by a decrypting device in decryption of the encryption-resultant contents information, and the algorithm identification information is for identifying the one among the plurality of predetermined key generation algorithms which should be used by the decrypting device in response to a reference table holding the plurality of predetermined key generation algorithms.

6. (Currently amended) A recording medium loaded with encryption-resultant contents information, encryption-resultant first-key base information, initial-value information, and algorithm identification information, wherein the encryption-resultant contents information and the encryption-resultant first-key base information are generated by the steps of generating a first-key signal representative of a first key from first-key base information being a base of the first key; encrypting contents information into encryption-resultant contents information in response to the first-key signal; generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to one selected from a plurality of predetermined key generation algorithms; and encrypting at least a part of the first-key base information into encryption-resultant first-key base information in response to the second-key signal; and wherein the algorithm identification information is for identifying the one selected from the plurality of predetermined key generation algorithms~~.~~ ; and wherein it is previously decided that the

plurality of predetermined key generation algorithms are usable by a decrypting device in decryption of the encryption-resultant contents information, and the algorithm identification information is for identifying the one among the plurality of predetermined key generation algorithms which should be used by the decrypting device in response to a reference table holding the plurality of predetermined key generation algorithms.

7. (Original) An apparatus as recited in claim 3, wherein the means for generating the second-key signal comprises a linear feedback shift register using a specified irreducible primitive polynomial.

8-14. (Canceled)

15. (Currently amended) A method of decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a first-key signal representative of a first key from first-key base information being a base of the first key; encrypting contents information into encryption-resultant contents information in response to the first-key signal; generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to one selected from a plurality of predetermined key generation algorithms; and encrypting at least a part of the first-key base information into encryption-resultant first-key base information in response to the second-key signal; the method comprising the steps of:

identifying the one selected from the plurality of predetermined key generation algorithms in response to algorithm identification information for identifying the one selected from the plurality of predetermined key generation algorithms;

generating a second-key signal representative of a second key on the basis of the initial-value information and the identified key generation algorithm;

decrypting encryption-resultant first-key base information into original first-key base information in response to the second-key signal;

generating a first-key signal representative of a first key from the original first-key base information; and decrypting encryption-resultant contents information into original contents information in response to the first-key signal~~.~~;

wherein it is previously decided that the plurality of predetermined key generation algorithms are usable by a decrypting device in decryption of the encryption-resultant contents information, and the plurality of predetermined key generation algorithms are stored in a reference table and the identifying step includes identifying the one among the plurality of predetermined key generation algorithms which should be used by the decrypting device in response to the algorithm identification information by referring to the reference table.

16. (Currently amended) An apparatus for decrypting encryption-resultant contents information generated by an encrypting side which implements the steps of generating a first-key signal representative of a first key from first-key base information being a base of the first key; encrypting contents information into encryption-resultant contents information in response to the first-key signal; generating a second-key signal representative of a second key on the basis of initial-value information of a given initial value according to one selected from a plurality of predetermined key generation algorithms; and encrypting at least a part of the first-key base information into encryption-resultant first-key base information in response to the second-key signal; the apparatus comprising:

a reference table storing the plurality of predetermined key generation algorithms identifiable by algorithm identification information, wherein it is previously decided that the plurality of predetermined key generation algorithms are usable by a decrypting device in decryption of the encryption-resultant contents information;

means for identifying the one selected from the plurality of predetermined key generation algorithms in response to the algorithm identification information by referring to the reference table ~~for identifying the one selected from the plurality of predetermined key generation algorithms~~;

means for generating a second-key signal representative of a second key on the basis of the initial-value information and the identified key generation algorithm;

means for decrypting encryption-resultant first-key base information into original first-key base information in response to the second-key signal;

means for generating a first-key signal representative of a first key from the original first-key base information; and

means for decrypting encryption-resultant contents information into original contents information in response to the first-key signal.

17. (Canceled)

18. (Original) An apparatus as recited in claim 17, wherein the means for generating the second-key signal comprises a linear feedback shift register having a feedback object position which is set in accordance with a primitive polynomial in the identified key generation algorithm.

19-22. (Canceled)